SYSTEM

Bintec Benutzerhandbuch - VPN Access Reihe
Version 1.1

Ziel und Zweck Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Bintec-Gateways ab Software-Release 7.1.4. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter www.bintec.de.

Haftung Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie **Release Notes** für Bintec-Gateways finden Sie unter www.bintec.de.

Als Multiprotokollgateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Richtlinien und Normen Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.bintec.de.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

Telefon: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
Frankreich

Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr



1 Menü System

Im Folgenden werden die Felder des Menüs *SYSTEM* beschrieben.

```
VPN Access 25 Setup Tool                          Bintec Access Networks GmbH
[SYSTEM]: Change System Parameters                                  MyGateway

 System Name                  vpn25
 Local PPP ID (default)       vpn25
 Location                     European Union
 Contact                      BINTEC


 Syslog output on serial console      no
 Message level for the syslog table   info
 Maximum Number of Syslog Entries     50

 External Activity Monitor >
 External System Logging >
 Schedule & Monitor >
 Password settings >
 Time and Date >

          SAVE                      CANCEL
```

Im Menü ***SYSTEM*** werden u.a. die grundlegenden Systemdaten Ihres Gateways eingetragen.

Das Menü ***SYSTEM*** besteht aus folgenden Feldern:

Feld	Wert
System Name	Definiert den Systemnamen Ihres Gateways; wird auch als PPP-Host-Name benutzt. Erscheint beim Einloggen auf dem Gerät als Eingabe-Prompt. Als Defaultwert ist der Gerätetyp voreingestellt.
Local PPP ID (default)	Diese Eintragung ist zur Identifizierung Ihres Gateways nötig, wenn das entfernte Gateway die PPP ID anfordert, bevor sich das Gateway der Gegenstelle identifiziert hat. Als Defaultwert ist der Gerätetyp eingestellt.

Feld	Wert
Location	Gibt an, wo sich Ihr Gateway befindet. Defaultwert: *European Union* Wird z.B. auf der HTML-Systeminfo-Seite oder in der Login-Meldung angezeigt.
Contact	Gibt die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden. Defaultwert: *BINTEC* Wir z.B. auf der HTML-Systeminfo-Seite angezeigt.
Syslog output on serial console	Ermöglicht die Anzeige von Syslog Messages auf dem mit der seriellen Schnittstelle des **VPN Access** Gateway verbundenen Rechner. Verwenden Sie diese Einstellung nur, wenn Sie eine Fehleranalyse machen, da massiver Output über die serielle Konsole sich auf den Durchsatz der anderen Schnittstellen auswirkt. Verwenden Sie im Normalfall das ***EXTERNAL SYSTEM LOGGING.*** Mögliche Werte: ■ *yes* ■ *no* (Defaultwert)

Feld	Wert
Message level for the syslog table	Spezifiziert die Priorität der intern aufzuzeichnenden Syslog Messages. Mögliche Werte: ■ *emerg*: Emergency Messages (höchste Priorität) ■ *alert*: Alert Messages ■ *crit*: Critical Messages ■ *err*: Error Messages ■ *warning*: Warning Messages ■ *notice*: Notice Messages ■ *info*: Info Messages (Defaultwert) ■ *debug*: Debug Messages (niedrigste Priorität) Nur Syslog Messages mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass beim Syslog-Level *debug* sämtliche erzeugten Meldungen aufgezeichnet werden.
Maximum Number of Syslog Entries	Maximale Anzahl an Syslog Messages, die auf dem **VPN Access** Gateway intern gespeichert werden (Wertebereich: *0* ... *1000*). Defaultwert: *50* Sie können die gespeicherten Meldungen im Setup Tool unter ***MONITORING AND DEBUGGING* ➜ *MESSAGES*** anzeigen lassen.

Tabelle 1-1: Felder im Menü ***SYSTEM***

2 Untermenü External Activity Monitor

Im Folgenden werden die Felder des Untermenüs *EXTERNAL ACTIVITY MONITOR* beschrieben.

```
VPN Access 25 Setup Tool                       Bintec Access Networks GmbH
[SYSTEM]: [ACTIVMON]: External Activity Monitor                  MyGateway


  Client IP Address                         255.255.255.255
  Client UDP Port                           2107
  Type                                      off
  Update Interval (sec)                     5



            SAVE                                 CANCEL

```

Im Menü ***SYSTEM*** ➜ ***EXTERNAL ACTIVITY MONITOR*** finden Sie die Einstellungen, die nötig sind, um Ihr **VPN Access** Gateway mit dem Windows-Tool Activity Monitor (Bestandteil von **BRICKware for Windows**) überwachen zu können.

Zweck Mit dem **Activity Monitor** können Windows-Nutzer die Aktivitäten des Gateways überwachen. Wichtige Informationen über den Status von physikalischen Schnittstellen (z. B. ISDN-Leitung) und virtuellen Schnittstellen (z. B. WAN Partner) sind leicht mit einem Tool erreichbar. Ein permanenter Überblick über die Auslastung der Schnittstellen des Gateways ist möglich.

Funktionsweise Ein Status-Daemon sammelt Informationen über das Gateway und überträgt sie in Form von UDP-Paketen zur Broadcast-Adresse der ersten LAN-Schnittstelle (Standardeinstellung) oder zu einer explizit eingetragenen IP-Adresse. Ein Paket pro Zeitintervall, das individuell einstellbar ist auf Werte von 1 - 60 Sekunden, wird gesendet. Bis zu 100 physikalische und virtuelle Schnittstellen können überwacht werden, soweit die Paketgröße von 4096 Bytes nicht überschritten wird. Der Activity Monitor auf Ihrem PC empfängt die Pakete und kann die enthaltenen Informationen je nach Konfiguration auf verschiedene Arten darstellen.

Um den **Activity Monitor** zu aktivieren, müssen Sie:

- das/die zu überwachende(n) Gateway(s) entsprechend konfigurieren,
- die Windows-Anwendung auf Ihrem PC starten und konfigurieren (siehe **BRICKware for Windows**).



Warnung!

Vermeiden Sie es, als ***CLIENT IP ADDRESS*** einen WAN Partner einzustellen, der über eine ISDN-Wählverbindung erreichbar ist. Dieses kann durch häufiges Aufbauen von ISDN-Verbindungen zu hohen Kosten führen.

Das Menü ***EXTERNAL ACTIVITY MONITOR*** besteht aus folgenden Feldern:

Feld	Wert
Client IP Address	IP-Adresse, zu der das Gateway die UDP Pakete schickt. Mit dem Standardwert *255.255.255.255* wird die Broadcast-Adresse der ersten LAN-Schnittstelle verwendet.
Client UDP Port	Port-Nummer für den Bintec Activity Monitor (Defaultwert: *2107*, registriert durch IANA - Internet Assigned Numbers Authority).
Type	Art der Informationen, die mit den UDP-Paketen zur Windows-Anwendung geschickt werden. Mögliche Werte: ■ *off*: deaktiviert **Activity Monitor** (Defaultwert) ■ *physical*: nur Informationen über physikalische Schnittstellen ■ *physical_virt*: Informationen über physikalische und virtuelle Schnittstellen
Update Interval (sec)	Update-Intervall in Sekunden. Mögliche Werte: *0* bis *60* (Defaultwert: *5*). Der Wert *0* deaktiviert die Funktion.

Tabelle 2-1: Felder im Menü ***EXTERNAL ACTIVITY MONITOR***

3 Untermenü External System Logging

Im Folgenden werden die Felder des Untermenüs *EXTERNAL SYSTEM LOGGING* beschrieben.

Im Menü ***SYSTEM*** ➜ ***EXTERNAL SYSTEM LOGGING*** werden die Log Host Einstellungen angezeigt.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SYSTEM][LOGGING][ADD]                                        MyGateway

     Log Host
     Level                      info
     Facility                   local0
     Type                       all
     Timestamp                  none

           SAVE                               CANCEL
```

Ereignisse in den verschiedenen Subsystemen des Gateways (z. B.: ➤➤ **ISDN**, ➤➤ **PPP** usw.) werden in Form von Syslog Messages (system logging messages) protokolliert. (Siehe “Menü System” auf Seite 3.) Je nach eingestelltem Level (acht Stufen von *emerg* über *info* bis *debug*) werden dabei weniger oder mehr Meldungen sichtbar.

Zusätzlich zu den intern auf dem Gateway protokollierten Daten können und sollten alle Informationen zur Speicherung und Weiterverarbeitung zusätzlich an einen oder mehrere externe Rechner weitergeleitet werden, z. B. an den Rechner des Systemadministrators. Auf dem Gateway intern gespeicherte Syslog Messages gehen bei einem Neustart verloren.



Warnung!

Vermeiden Sie es, Syslog Messages auf Log Hosts weiterzuleiten, die über eine Wählverbindung erreicht werden. Dies kann zu erheblichen Kosten führen.

Achten Sie darauf, die Syslog Messages nur an einen sicheren Rechner weiterzuleiten. Kontrollieren Sie die Daten regelmäßig und achten Sie darauf, dass jederzeit ausreichend freie Kapazität auf der Festplatte des Rechners zur Verfügung steht.

Syslog-Daemon

Die Erfassung der Syslog Messages wird von allen Unix-Betriebssystemen unterstützt. Für Windows-Rechner ist in den **DIME Tools** ein Syslog-Daemon enthalten, der die Daten aufzeichnen und je nach Inhalt auf verschiedene Dateien verteilen kann (siehe **BRICKware for Windows**).

Die Einstellungen für das externe Speichern von Syslog Messages erfolgen in ***SYSTEM*** ➜ ***EXTERNAL SYSTEM LOGGING*** ➜ ***ADD/EDIT***.

Das Menü ***EXTERNAL SYSTEM LOGGING*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Log Host	➤➤ **IP-Adresse** des Hosts, zu dem Syslog Messages weitergeleitet werden.
Level	Priorität der zum ***LOG HOST*** zu schickenden Syslog Messages. Die möglichen Werte entsprechen denen in “Message level for the syslog table” auf Seite 5 Nur Syslog Messages mit gleicher oder höherer Priorität als angegeben werden an den ***LOG HOST*** gesendet, d.h. dass beim Syslog-***LEVEL*** *debug* sämtliche erzeugten Meldungen an den ***LOG HOST*** weitergeleitet werden.
Facility	Syslog-Facility auf ***LOG HOST***. Nur erforderlich, wenn der ***LOG HOST*** ein Unix-Rechner ist. Mögliche Werte: *local0 - 7* (Defaultwert *local0*).

Feld	Wert
Type	Nachrichtentyp. Mögliche Werte: ■ *all*: Alle Messages (Defaultwert) ■ *system*: Syslog Messages außer ➤➤ **Accounting**-Messages ■ *accounting*: Accounting-Messages
Timestamp	Format der Systemzeit des **VPN Access** Gateway im Syslog. Mögliche Werte: ■ *all*: Systemzeit mit Datum ■ *time*: Systemzeit ohne Datum ■ *none*: keine Systemzeitangabe (Defaultwert)

Tabelle 3-1: Felder im Menü ***EXTERNAL SYSTEM LOGGING***

4 Untermenü Schedule & Monitor

Im Folgenden werden die Felder des Untermenüs *SCHEDULE & MONITOR* beschrieben.

Über das Menü ***SCHEDULE & MONITOR*** gelangen Sie in weitere Untermenüs:

- ***KEEPALIVE MONITORING (HOSTS & IFC)***
- ***EVENT SCHEDULER (TIME & SNMP)***

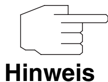
4.1 Untermenü Keepalive Monitoring (Hosts & Ifc)

Im Menü ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***KEEPALIVE MONITORING (HOSTS & IFC)*** finden Sie Einstellungen für die Funktion "Keepalive Monitoring".

Beispielszenario

Wenn Sie zwei (oder mehrere) LANs über eine Wählverbindung gekoppelt haben – z. B. das LAN der Firmenzentrale mit dem LAN einer Filiale – befindet sich häufig ein zentraler Server im LAN der Firmenzentrale. Wenn dieser zentrale Server so konfiguriert ist, dass er regelmäßig WAN-Verbindungen zum Gateway im LAN der Filiale aufbaut, z. B. um Daten zu aktualisieren, dann sind diese Verbindungen überflüssig (aber nicht kostenlos), wenn keiner der Hosts in der Filiale erreichbar ist, z. B. weil alle Rechner ausgeschaltet sind. Da erst nach dem Aufbau der Verbindung festgestellt werden kann, dass die Hosts nicht erreichbar sind, entstehen Kosten für den Rufenden, also für die Firmenzentrale.

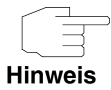
Mit der Funktion "Keepalive Monitoring" können Sie das Gateway in der Filiale so konfigurieren, dass unnötige WAN-Verbindungen von der Firmenzentrale zur Filiale vermieden werden. In regelmäßigen, einstellbaren Abständen überprüft das Gateway der Filiale, ob die zu überwachenden Hosts in seinem LAN erreichbar sind. Wenn nach drei aufeinanderfolgenden Versuchen keiner der zu überprüfenden Hosts auf eine entsprechende Anfrage antwortet, deaktiviert das Gateway die Schnittstelle zum WAN Partner "Firmenzentrale". Rufe seitens der Firmenzentrale an nicht erreichbare Hosts werden gar nicht erst angenommen, und es entstehen keine Kosten.



Hinweis

In manchen Ländern (z. B. Schweiz) können trotz Nutzung von Keepalive Monitoring Kosten für diese vergeblichen Einwahlversuche anfallen.

Wenn alle Rechner im LAN der Filiale inaktiv waren, wird beim Einschalten eines zu überwachenden Rechners nicht automatisch sofort eine Verbindung zur Firmenzentrale aufgebaut. Erst wenn das Gateway in der Filiale die Erreichbarkeit eines Rechners registriert hat, wird die Schnittstelle zum WAN Partner "Firmenzentrale" aktiviert, und ein Verbindungsaufbau durch die Firmenzentrale ist möglich. Wieviel Zeit vergeht, bis das Gateway die erneute Erreichbarkeit signalisiert, ist abhängig vom eingestellten Überwachungsintervall (***INTERVAL***).



Hinweis

Die entsprechende Gegenstelle, also z. B. die Firmenzentrale, muss auf dem Gateway der Filiale per CLID (Calling Line Identification) identifiziert werden können. Wenn dies nicht der Fall ist, ist der beschriebene Nutzeffekt von "Keepalive Monitoring" nicht gegeben.

Keepalive Monitoring kann auf dem Gateway nicht für WAN Partner eingerichtet werden, die über einen RADIUS-Server authentifiziert werden!

In ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***KEEPALIVE MONITORING*** sind die *Hosts* und *Interfaces* aufgelistet, die per Keepalive Monitoring überwacht werden. Unter ***STATE*** ist dabei die Erreichbarkeit der Hosts aufgelistet: *alive*, wenn der Host bei der letzten Überprüfung erreichbar war, *down*, wenn er nicht erreichbar war.

In dem Menü ***WHAT TO MONITOR:*** wird eingestellt, ob die Konfiguration für *hosts* oder *interfaces* vorgenommen wird.

WHAT TO MONITOR: HOSTS

```
VPN Access 25 Setup Tool                         Bintec Access Networks GmbH
[SYSTEM][KEEPALIVE MONITORING][ADD]: Host Monitoring              MyGateway


  Group                          0
  IPAddress
  Interval                       300
  Source IP
  DownAction                     down
  FirstIfIndex                   10001
  Range                          4999


            SAVE                                CANCEL

```

Wenn *hosts* gewählt wurde, besteht das Menü ***KEEPALIVE MONITORING*** ➜ ***ADD/EDIT*** aus folgenden Feldern:

Feld	Wert
Group	Definiert eine Gruppe von Hosts, deren Erreichbarkeit vom **VPN Access** Gateway überwacht werden soll. Jeder zu überwachende Host wird einer Gruppe zugeordnet. Insgesamt können 256 Gruppen angelegt werden. Mögliche Werte: *0* (Defaultwert) ... *255.*
IPAddress	Definiert einen Host, der vom **VPN Access** Gateway überwacht werden soll.
Interval	Definiert ein Zeitintervall in Sekunden, welches zur Überprüfung der Erreichbarkeit von Hosts verwendet werden soll. Mögliche Werte: *1 ... 65536* (Defaultwert: *300* s). Innerhalb einer Gruppe wird das kleinste ***INTERVAL*** der Gruppenmitglieder verwendet.
Source IP	Diejenige IP-Adresse, die das Gateway als Quelladresse des Pakets verwendet, das an den zu überwachenden Host gesendet wird.

Feld	Wert
DownAction	Definiert, wie der Status der unter ***FirstIfIndex*** und ***Range*** festgelegten **VPN Access** Gateway-Schnittstellen gesetzt wird, wenn alle Hosts einer Gruppe nicht erreichbar sind. Mögliche Werte: ■ *down*: Schnittstellen werden deaktiviert, d.h. Admin-Status wird auf *down* gesetzt (Defaultwert) ■ *none*: keine Aktion, d.h. Admin-Status wird auf *up* gesetzt ■ *up*: Schnittstellen werden aktiviert Wenn mindestens ein Host einer Gruppe wieder erreichbar ist, wird der Status der Schnittstellen wieder auf den ursprünglichen Wert gesetzt. Beachte: Die ***DownAction*** innerhalb einer Gruppe muss identisch konfiguriert werden!
FirstIfIndex	Definiert die erste Schnittstelle eines Schnittstellen-Bereiches auf dem **VPN Access** Gateway, für welche die unter ***DownAction*** festgelegte Aktion (*down* oder *up*) ausgeführt werden soll. Mögliche Werte: *100 .. 65536* Defaultwert: *10001* Für Wählverbindungen zu WAN Partnern sind Schnittstellen mit Indizes von *10001* bis *14999* vorgesehen. Die Indizes der Schnittstellen können Sie z.B. mit dem Befehl `ifstat` anzeigen lassen.

Feld	Wert
Range	Definiert den Bereich von Schnittstellen auf dem **VPN Access** Gateway, für welche die unter ***DownAction*** festgelegte Aktion ausgeführt werden soll. Defaultwert: *4999* Wenn Sie ***FirstIfIndex*** = *10001* und ***Range*** = *0* einstellen, ist nur die Schnittstelle mit dem Index *10001* betroffen. Wenn Sie ***FirstIfIndex*** = *10001* und ***Range*** = *19* einstellen, sind die Schnittstellen mit den Indizes *10001* bis *10020* betroffen.

Tabelle 4-1: Felder im Menü ***Keepalive Monitoring*** *hosts*

What to monitor*: *Interfaces

```
VVPN Access 25 Setup Tool                         Bintec Access Networks GmbH
[SYSTEM][KEEPALIVE MONITORING][ADD]: Interface Monitoring      MyGateway

  Interface                    0
  Trigger                      down
  Action                       none


            SAVE                                CANCEL
```

Wenn in ***What to monitor:*** *interfaces* gewählt wurde, besteht das Menü ***Keepalive Monitoring*** ➜ ***ADD/EDIT*** aus folgenden Feldern:

Feld	Wert
Interface	Definiert das zu überwachende Interface auf dem **VPN Access** Gateway. Hier wird der ***Index*** der Schnittstelle eingetragen. Der ***Index*** wird z.B. mit dem Befehl `ifstat` ermittelt. Defaultwert: *0*

Feld	Wert
Trigger	Definiert den Status von ***INTERFACE***, der eine bestimmte ***ACTION*** auslöst. Mögliche Werte: ■ down: Interface ist deaktiviert (Defaultwert) ■ up: Interface ist aktiviert
Action	Definiert die Aktion, die auf den in ***TRIGGER*** definierten Status folgen soll. Die Aktion wird auf den Schnittstellenbereich von ***FIRSTIFINDEX*** und ***FIRSTIFINDEX*** + ***RANGE*** ausgeführt. Mögliche Werte: ■ *none:* keine Aktion (Defaultwert) ■ *down*: Deaktivierung der Schnittstelle(n) ■ *up*: Aktivierung der Schnittstelle(n)
FirstIfIndex	Definiert die erste Schnittstelle eines Schnittstellen-Bereiches auf dem **VPN Access** Gateway, für welche die unter ***DOWNACTION*** festgelegte Aktion (*down* oder *up*) ausgeführt werden soll. Mögliche Werte: *100 .. 65536* Defaultwert: *10001* Für Wählverbindungen zu WAN Partnern sind Schnittstellen mit Indizes von *10001* bis *14999* vorgesehen. Die Indizes der Schnittstellen finden Sie z.B. mit dem Befehl `ifstat`.

Feld	Wert
Range	Definiert den Bereich von Schnittstellen auf dem **VPN Access** Gateway, für welche die unter ***ACTION*** festgelegte Aktion ausgeführt werden soll. Wenn Sie ***FIRSTIFINDEX*** = *10001* und ***RANGE*** = *0* einstellen, ist nur die Schnittstelle mit dem Index *10001* betroffen. Wenn Sie ***FIRSTIFINDEX*** = *10001* und ***RANGE*** = *4999* (Defaultwert) einstellen, sind die Schnittstellen mit den Indizes *10001* bis *14999* betroffen.

Tabelle 4-2: Felder im Menü ***KEEPALIVE MONITORING*** *interfaces*

4.2 Untermenü Event Scheduler (Time & SNMP)

Ab Systemsoftware 7.1.4 verfügt Ihr Gateway über einen Event Scheduler, mittels dessen es möglich ist, beliebige Einträge in die MIB vorzunehmen, sobald ein bestimmtes (ebenfalls frei konfigurierbares) Ereignis eintritt.

Abgesehen von voreingestellten und einfach zu konfigurierenden Standardanwendungen wie zeit- oder volumengesteuerte Aktivierung bzw. Deaktivierung von Interfaces, ermöglicht es der Event Scheduler, beliebig auf MIB-Parameter zuzugreifen. Dadurch können beliebige Ereignisse in der MIB als Auslöser ebenfalls beliebiger Aktionen definiert werden.



Achtung!

Die Konfiguration der nicht voreingestellten Aktionen erfordert umfangreiches Wissen über die Funktionsweise der Bintec Gateways. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration z. B. auf Ihrem PC.

Die Konfiguration des Event Scheduler erfolgt im Menü ***System*** ➜ ***Schedule & Monitor*** ➜ ***Event Scheduler (Time & SNMP)***:

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SYSTEM][SCHEDULED]: Event Schedule                           MyGateway

                  Event Scheduler            disabled

                  Schedule Events >
                  Schedule Commands >

                  SAVE                  CANCEL
```

Im Feld ***Event Scheduler*** aktivieren (*enabled*) oder deaktivieren (*disabled*) Sie den Scheduler, per Default ist er deaktiviert. Bei Aktivierung des ***Event Scheduler*** wird der Schedule-Intervall per default auf *300s* gesetzt. Im Menü ***Schedule Events*** konfigurieren Sie die Ereignisse, die eine bestimmte Aktion auf dem Gateway auslösen sollen, im Menü ***Schedule Commands*** die auszuführenden Aktionen. Die Auslöser (Events) können zu Ereignis-Ketten verknüpft werden, so dass auch komplexe Bedingungen für das Auslösen einer Aktion erstellt werden können.

4.2.1 Konfiguration der Auslöser (Events)

Die Ereignisse, die eine entsprechende Aktion auslösen, werden im Menü *System* ➜ *Schedule & Monitor* ➜ *Event Scheduler (Time & SNMP)* ➜ *Schedule Events* ➜ *ADD/EDIT* erstellt bzw. editiert.

Standardmäßig öffnet sich das Menü mit der Maske zur Konfiguration eines Ereignisses vom Typ *time*:

```
VPN Access 25 Setup Tool                           Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_EVT][ADD]: Scheduler Events            MyGateway

     Index        1        Description
     NextIndex    none
     Type         time


     Condition             dayly
       Start time  (hh:mm)
       End time    (hh:mm)

     Status                notavail

                    SAVE                          CANCEL

```

Wenn Sie ***Type*** = *value* auswählen, ändert sich das Menü wie folgt:

```
VPN Access 25 Setup Tool                           Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_EVT][ADD]: Scheduler Events            MyGateway

     Index        1        Description
     NextIndex    none
     Type         value

     Monitored event       user defined
       Table
       Variable
       Index variable
       Index value

     Condition             range
       Compare value
       End value

     Status                notavail

                    SAVE                          CANCEL

```

Je nach Einstellung enthält das Menü folgende Felder:

Feld	Wert
Index	Das Gateway vergibt automatisch eine Index-Nummer für den Eintrag. Der Wert kann aber auch editiert werden. Es stehen alle Werte von *1* bis *65535* zur Verfügung.
Description	Hier geben Sie eine beliebige Bezeichnung für das Ereignis ein. Die maximale Länge des Eintrags beträgt 30 Zeichen.
NextIndex	Hier wählen Sie aus den bereits vorhanden Einträgen aus, welcher Eintrag dem aktuellen in einer Ereigniskette folgen soll. Die Einträge einer Ereigniskette bilden eine komplexe Bedingung für eine auszuführende Aktion. Wie die Ereigniskette zu einer Aktion führt, wird im Menü ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***EVENT SCHEDULER (TIME & SNMP)*** ➜ ***SCHEDULE COMMANDS*** konfiguriert.
Type	Hier wählen Sie, welchen Typ von Ereignis Sie als Auslöser einer Aktion definieren wollen: Zur Verfügung stehen: ■ *time* - Die Aktion wird zu bestimmten Zeiten ausgelöst (Defaultwert). Bitte achten Sie auf die korrekte Systemzeit auf dem Gateway! ■ *value* - Die Aktion wird ausgelöst, sobald eine MIB-Variable einen bestimmten Wert annimmt.

Feld	Wert
Monitored event	Nur für **TYPE** = *value*. Hier können Sie zwischen unterschiedlichen Ereignissen wählen. Zur Verfügung stehen: ■ *user defined* - Sie können frei wählen, auf welchen Wert welcher MIB-Variablen der Scheduler mit einer Aktion reagieren soll (Defaultwert). ■ *WAN interface total charge* - Ein Auslöser wird aktiv, wenn auf einem WAN-Interface (die Auswahl des Interfaces erfolgt bei der Konfiguration der Aktion) ein bestimmtes Gesamtkostenlimit aller Verbindungen erreicht wurde. Dazu ist es notwendig, dass dem Gateway vom Provider Gebühreninformationen übertragen werden. ■ *WAN interface total duration* - Ein Auslöser wird aktiv, wenn die Gesamtdauer aller Verbindungen eines WAN-Interfaces (in Sekunden) einen bestimmten Wert erreicht hat. ■ *WAN interface total RX traffic* - Ein Auslöser wird aktiv, wenn ein WAN-Interface eine bestimmte Gesamtmenge an Daten aller Verbindungen (in Bytes) empfangen hat. ■ *WAN interface total TX traffic* - Ein Auslöser wird aktiv, wenn ein WAN-Interface eine bestimmte Gesamtmenge an Daten aller Verbindungen (in Bytes) gesendet hat.

Feld	Wert
Table	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie den Namen der MIB-Tabelle an, in der sich die MIB-Variable befindet, die für den Auslöser verwendet werden soll, z. B. ***BIBOPPPSTATTABLE***.
Variable	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie den Namen der MIB-Variable ein, die für den Auslöser verwendet werden soll, z. B. ***TOTALDURATION***.
Index variable	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie den Namen der Indexvariable der zuvor definierten MIB-Tabelle ein. Dies ist in einer beliebigen MIB-Tabelle diejenige Variable, die in der Tabellenansicht mit einem Asterisk (*) markiert ist, z. B. ***PPPTYPE***. Die Einträge in einer MIB-Tabelle werden intern indiziert. In der normalen Tabellenansicht wird diese Indizierung nicht angezeigt. Geben Sie auf der Shell `y` ein, um den Tabellenmodus zu deaktivieren. Wenn Sie nun z. B. `pppTable` eingeben, werden die Einträge in einem Format aufgelistet, in dem die Indizierung sichtbar ist (z. B. ***BIBOPPPTYPE.1.1(RW): ISDN_DIALUP***). Aus der Kombination der Indexvariablen und ihres Wertes (inklusive des internen Indexes) ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.
Index value	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie den Wert ein, den ***INDEX VARIABLE*** für den Tabelleneintrag hat, der für den Auslöser verwendet werden soll, z. B. ***ISDN_DIALUP***.

Feld	Wert
Condition	Für ***Type*** = *time*: ■ *daily* - Der Auslöser wird täglich aktiv (Defaultwert). ■ *<Wochentag>* - Der Auslöser wird wiederkehrend an einem bestimmten Wochentag aktiv. ■ *mon_fri* - Der Auslöser wird täglich von Montag bis Freitag aktiv. ■ *sat_sun* - Der Auslöser wird wiederkehrend nur Samstags und Sonntags aktiv. ■ *day<1 .. 31>* - Der Auslöser wird wiederkehrend an einem bestimmten Tag des Monats aktiv. Für ***Type*** = *value*: ■ *range* - Der Auslöser wird aktiv, wenn der Wert der Variablen innerhalb eines bestimmten Wertebereichs liegt (Defaultwert). ■ *greater* - Der Auslöser wird aktiv, wenn der Wert der Variablen einen bestimmten Wert übersteigt. ■ *equal* - Der Auslöser wird aktiv, wenn der Wert der Variablen einen bestimmten Wert annimmt. ■ *less* - Die Aktion wird aktiv, wenn der Wert der Variablen unter einem bestimmten Wert ist. ■ *notequal* - Der Auslöser wird aktiv, wenn der Wert der Variablen einen bestimmten Wert nicht annimmt.

Feld	Wert
Compare value	Wert, mit dem der Wert von ***Variable*** unter der in ***Condition*** definierten Bedingung verglichen wird. Wenn ***Condition*** = *range*, so ist dies der Startwert des Wertebereichs.
End value	Wenn ***Condition*** = *range*, so ist dies der Endwert des Wertebereichs.
Start time (hh:mm)	Nur für ***Type*** = *time*. Hier geben Sie den Zeitpunkt ein, an dem der Auslöser aktiviert werden soll.
End time (hh:mm)	Nur für ***Type*** = *time*. Hier geben Sie den Zeitpunkt ein, an dem der Auslöser deaktiviert werden soll. Wenn Sie keine ***End Time*** eingeben, wird der Auslöser einmalig aktiviert und sofort wieder deaktiviert. Dies ist nützlich um eine kurzzeitige Aktion auszuführen, z. B. um nachts eine DSL-Verbindung zu trennen.
Status	Dieses Feld kann nicht editiert werden und zeigt den Status des Auslösers an. Mögliche Werte sind: ■ *active* - Der Auslöser ist derzeit aktiv. ■ *inactive* - Der Auslöser ist inaktiv. ■ *notavail* - Der Status kann nicht festgestellt werden, z. B. wenn der Scheduler nicht aktiviert ist. ■ *error* - Es ist ein Fehler aufgetreten, die Konfiguration des Auslösers ist nicht konsistent.

Tabelle 4-3: ***System ➜ Schedule & Monitor ➜ Event Scheduler (Time & SNMP) ➜ Schedule Events ➜ ADD/EDIT***

4.2.2 Konfiguration der Aktion (Command)

Welche Aktion ausgeführt wird, sobald eines der als Auslöser konfigurierten Ereignisse eintritt, wird im Menü *SYSTEM* ➜ *SCHEDULE & MONITOR* ➜ *EVENT SCHEDULER (TIME & SNMP)* ➜ *SCHEDULE COMMANDS* ➜ *ADD/EDIT* erstellt bzw. editiert.

Standardmäßig öffnet sich das Menü zur Konfiguration der Aktionen wie folgt:

```
VPN Access 25 Setup Tool                       Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_CMD][ADD]: Scheduler Commands         MyGateway

     Index        1        Description
     Mode                  enable
     1. Event Index        none
     Eventlist Condition   all

     Execute command       disable interface
     Interface             en1-0


     Notify                all

     Status    notavail       Last Change    01/01/1970  0:00:00

                  SAVE                          CANCEL

```

Wenn Sie für das Feld ***Execute Command*** den Wert *user defined* auswählen, ändert sich das Menü wie folgt:

```
VPN Access 25 Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_CMD][ADD]: Scheduler Commands        MyGateway


     Index        1          Description
     Mode                    enable
     1. Event Index          none
     Eventlist Condition     all

     Execute command         user defined
       Table
       Variable
       Index variable
       Index value
       Set value active
           value inactive
     Notify                  all

     Status    notavail        Last Change     01/01/1970   0:00:00

                    SAVE                              CANCEL

```

Je nach gewählter Einstellung enthält das Menü folgende Felder:

Feld	Wert
Index	Das Gateway vergibt automatisch eine Index-Nummer für den Eintrag. Der Wert kann aber auch editiert werden. Es stehen alle Werte von *1* bis *65535* zur Verfügung.
Description	Hier geben Sie eine beliebige Bezeichnung für die Aktion ein. Die maximale Länge des Eintrags beträgt 30 Zeichen.
Mode	Hier wählen Sie aus, ob die konfigurierte Aktion aktiv oder inaktiv sein soll. Zur Verfügung stehen: ■ *enable* (Defaultwert) ■ *disable*

Feld	Wert
1. Event Index	Hier legen Sie das erste Ereignis einer Ereigniskette fest. Die Ereigniskette wird erst von diesem Eintrag an aktiviert, vorhergehende Einträge werden ignoriert. Defaultwert ist *none*.
Eventlist Condition	Hier legen Sie fest, ob alle Einträge einer Ereigniskette zutreffen müssen, damit eine Aktion ausgeführt wird. Zur Verfügung stehen: ■ *all* - Alle Ereignisse einer Ereigniskette müssen auftreten, damit die Aktion ausgeführt wird (Defaultwert). ■ *one* - Mindestens eines der Ereignisse einer Ereigniskette muss auftreten, damit die Aktion ausgeführt wird. ■ *none* - Keines der Ereignisse einer Ereigniskette darf eintreten, damit die Aktion ausgeführt wird. ■ *one_not* - Mindestens eines der Ereignisse einer Ereigniskette darf nicht auftreten, damit die Aktion ausgeführt wird.

Feld	Wert
Execute command	Hier legen Sie die Aktion fest, die aufgrund eines Auslösers ausgeführt wird. Zur Verfügung stehen: ■ *disable interface* - Das im Feld ***Interface*** bestimmte Interface wird deaktiviert (sein ***AdminStatus*** wird auf *down* gesetzt, Defaultwert). ■ *enable interface* - Das im Feld ***Interface*** bestimmte Interface wird aktiviert (sein ***AdminStatus*** wird auf *up* gesetzt). ■ *user defined* - Die Aktion wird in den folgenden Feldern frei konfiguriert.
Interface	Hier wählen Sie aus, welches Interface aktiviert bzw. deaktiviert werden soll, wenn für ***Execute Command*** *disable interface* oder *enable interface* gewählt ist.
Table	Nur für ***Execute Command*** = *user defined*. Hier geben Sie die MIB-Tabelle ein, in der sich die zu setzende Variable befindet, z.B. *ifTable*.
Variable	Nur für ***Execute Command*** = *user defined*. Hier geben Sie die MIB-Variable ein, die gesetzt werden soll, z.B. *AdminStatus*.

Feld	Wert
Index variable	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie die Indexvariable der zuvor ausgewählten MIB-Tabelle ein. Dies ist in einer beliebigen MIB-Tabelle diejenige Variable, die in der Tabellenansicht mit einem Asterisk (*) markiert ist. Die Einträge in einer MIB-Tabelle werden intern indiziert. In der normalen Tabellenansicht wird diese Indizierung nicht angezeigt. Geben Sie auf der Shell `y` ein, um den Tabellenmodus zu deaktivieren. Wenn Sie nun z. B. `pppTable` eingeben, werden die Einträge in einem Format aufgelistet, in dem die Indizierung sichtbar ist (z. B. ***BIBOPPPTYPE.1.1(RW): ISDN_DIALUP***). Aus der Kombination der Indexvariablen und ihres Wertes (inklusive des internen Indexes) ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.
Index value	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie den Wert ein, den die Indexvariable für den Tabelleneintrag hat, der durch die Aktion geändert werden soll.
Set value active	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie den Wert ein, den ***VARIABLE*** durch die Aktion zugewiesen bekommen soll. Der Wert wird gesetzt, sobald ein entsprechender Auslöser aktiv wird und bleibt solange erhalten, bis der Auslöser wieder inaktiv wird.
value inactive	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie den Wert ein, den ***VARIABLE*** annimmt, sobald der Auslöser inaktiv wird. Dieser Wert wird der Variablen auch nach einem Neustart des Gateways zugewiesen oder wenn die Systemzeit nicht korrekt eingestellt ist.

Feld	Wert
Notify	Hier wählen Sie aus, welche Mechanismen verwendet werden, um über Aktionen zu informieren. Zur Verfügung stehen: ■ *all* (Defaultwert) - Es werden sowohl SNMP-Traps als auch Syslog-Meldungen erzeugt. ■ *snmptrap* - Es werden nur SNMP-Traps erzeugt. ■ *syslog* - Es werden nur Syslog-Meldungen erzeugt. ■ *none* - Es werden keine Meldungen erzeugt.
Status	Dieses Feld kann nicht editiert werden und zeigt den Status der Aktion an. Mögliche Werte sind: ■ *active* - Die Aktion ist derzeit aktiv. ■ *inactive* - Die Aktion ist inaktiv. ■ *notavail* - Der Status kann nicht festgestellt werden, z. B. wenn der Scheduler nicht aktiviert ist. ■ *error* - Es ist ein Fehler aufgetreten, die Konfiguration der Aktion ist nicht konsistent.
Last Change	Hier wird der Zeitpunkt der letzten Zustandsänderung angezeigt. Das Feld kann nicht editiert werden.

Tabelle 4-4: ***SYSTEM ➜ SCHEDULE & MONITOR ➜ EVENT SCHEDULER (TIME & SNMP) ➜ SCHEDULE COMMANDS ➜ ADD/EDIT***

5 Untermenü Password settings

Im Folgenden werden die Felder des Untermenüs *Password settings* beschrieben.

```
VPN Access 25 Setup Tool                       Bintec Access Networks GmbH
[SYSTEM][PASSWORDS]: Change System Passwords                    MyGateway

  admin Login Password/SNMP Community   ******
  read  Login Password/SNMP Community   ******
  write Login Password/SNMP Community   ******
  HTTP Server Password                  ******
  Activity Monitor Password             ******

           SAVE                                  CANCEL
```

Das Einstellen der Paßwörter gehört zu den grundlegenden Systemeinstellungen. (Nähere Informationen zu den Benutzerrechten der verschiedenen User finden Sie in **Zugang und Konfiguration**.)

Das Menü ***Password settings*** besteht aus folgenden Feldern:

Feld	Wert
admin Login Password/SNMP Community	Paßwort für Benutzername `admin`
read Login Password/SNMP Community	Paßwort für Benutzername `read`
write Login Password/SNMP Community	Paßwort für Benutzername `write`
HTTP Server Password	Paßwort für die HTTP-Statusseite Ihres Gateways
Activity Monitor Password	Paßwort für den ***Activity Monitor***

Tabelle 5-1: Felder im Menü ***Password settings***



Alle Bintec-Gateways werden mit gleichem Benutzernamen und Paßwort ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Paßwörter nicht geändert wurden.

Ändern Sie unbedingt die Paßwörter, um unberechtigten Zugriff auf das Gateway zu verhindern.

Solange das Paßwort nicht verändert wird, erscheint beim Einloggen der Warnhinweis: "Password not changed".

6 Untermenü Time and Date

Im Folgenden werden die Felder des Untermenüs *Time and Date* beschrieben.

```
VPN Access 25 Setup Tool                         Bintec Access Networks GmbH
[SYSTEM][TIME]: Set System Time and Date                           MyGateway

      Time is currently controlled by:            ISDN

      Current Time:
      Tue Jan 13   6:24:52  1970


      New Time: 06:23

      New Date: 01/13/1970

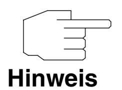


              SET                                 BACK
```

Systemzeit Die Systemzeit benötigen Sie u.a. für korrekte Zeitstempel bei Systemmeldungen, Accounting oder IPSec-Zertifikaten.

Sie können die Systemzeit:

- automatisch beziehen, z. B. über ISDN oder über einen Time-Server. Die entsprechende Konfiguration wird im Menü ***IP → Static Settings*** vorgenommen.
- manuell auf dem Gateway einstellen.



Hinweis

Wenn auf dem Gateway eine Methode zum automatischen Beziehen der Zeit festgelegt ist, haben die auf diese Weise erhaltenen Werte die höhere Priorität. eine evtl. manuell eingegebene Systemzeit wird überschrieben.

Im Menü ***System → Time and Date*** finden Sie Einstellungen zur manuellen Eingabe von Uhrzeit und Datum auf Ihrem Gateway.

Das Menü ***Time and Date*** besteht aus folgenden Feldern:

Feld	Wert
Time is currently controlled by:	Zeigt an, welche Einstellungen für ein automatisches Beziehen der Systemzeit unter ***IP*** ➜ ***Static Settings*** festgelegt sind.
Current Time:	Zeigt die aktuell auf dem **VPN Access** Gateway eingestellte Systemzeit an (Datum und Uhrzeit).
New Time:	Hier wird die neue Uhrzeit eingegeben, die das **VPN Access** Gateway verwenden soll (hh:mm).
New Date:	Hier wird das neue Datum eingegeben, das das **VPN Access** Gateway verwenden soll (mm/tt/jjjj).

Tabelle 6-1: Felder im Menü ***Time and Date***

Index: System